IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF
TEXAS WACO DIVISION

MONARCH NETWORKING SOLUTIONS LLC	§	**Civil Action No. 6:20-cv-381**
Plaintiff,	§	**Jury Trial Requested**
v.	§	
CISCO SYSTEMS, INC.; MERAKI LLC; DUO SECURITY, INC.	§	
Defendants.	§	

COMPLAINT FOR PATENT INFRINGEMENT

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff, Monarch Networking Solutions LLC ("Monarch"), for its Complaint against Defendants Cisco Systems, Inc. ("Cisco Systems"), Meraki LLC ("Meraki"), and Duo Security, Inc. ("Duo") (Cisco Systems, Meraki, and Duo are collectively referred to as "Cisco" herein), requests a trial by jury and alleges as follows upon actual knowledge with respect to itself and its own acts and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. This is an action for patent infringement. Monarch alleges that Cisco and certain of its subsidiaries infringe U.S. Patent No. 7,756,507 ("the '507 Patent" or the "Asserted Patent"), a copy of which is attached hereto as Exhibit A. Monarch also alleges that Cisco Systems' subsidiaries, Meraki and Duo, each individually infringe the '507 Patent.

2. Monarch alleges that Cisco Systems directly and indirectly infringes the Asserted Patent by making, using, offering for sale, selling and/or importing the Cisco Accused Products described below. Monarch further alleges that Cisco Systems induces and contributes to the infringement of others through the marketing and use of the Cisco Accused Products. Monarch seeks damages and other relief for Cisco System's infringement of the Asserted Patent.

3. Monarch alleges that Meraki directly and indirectly infringes the '507 Patent by making, using, offering for sale, selling and/or importing the products implementing the Meraki Cloud Hosted Authentication described below. Monarch further alleges that Meraki induces and contributes to the infringement of others through the marketing and use of the products implementing the Meraki Cloud Hosted Authentication. Monarch seeks damages and other relief for Meraki's infringement of the Asserted Patent.

4. Monarch alleges that Duo directly and indirectly infringes the '507 Patent by making, using, offering for sale, selling and/or importing the products implementing Duo Security described below. Monarch further alleges that Duo induces and contributes to the infringement of others through the use of the products implementing Duo Security. Monarch seeks damages and other relief for Duo's infringement of the Asserted Patent.

THE PARTIES

5. Monarch is a limited liability company organized under the laws of California with its principal place of business at 4 Park Plaza, Suite 550, Irvine, CA 92614.

6. Monarch is the assignee and owner of the '507 Patent through assignment as follows: 6/13/2019 assignment from Siemens Aktiengesellschaft to Acacia Research Group LLC; and 11/18/2019 assignment from Acacia Research Group LLC to Monarch Networking Solutions LLC.

7. On information and belief, Defendant Cisco Systems is a corporation organized under the laws of California with its principal place of business at 170 W. Tasman Dr., San Jose, CA 95134. Cisco Systems is registered to do business in the state of Texas. Cisco Systems has appointed the Prentice-Hall Corporation System, Inc., 211 E. 7th St., Suite 620, Austin, TX 78701 as its agent for service of process.

8. On information and belief, Cisco Systems maintains regular and established places of business and does business in Texas and in the Western District of Texas, *inter alia*, at its campuses at 12515-3 Research Park Loop, Austin, TX 78759, and at 18615 Tuscany Stone, San Antonio, TX 78258.

9. By registering to conduct business in Texas and by having facilities where it regularly conducts business in this District, Cisco Systems has a permanent and continuous presence in Texas and a regular and established place of business in the Western District of Texas.

10. On information and belief, Defendant Meraki is a limited liability company organized under the laws of Delaware with its principal place of business at 500 Terry A Francois Blvd., San Francisco, CA 94158. Meraki is registered to do business in the state of Texas. Defendant Meraki was acquired by and is a subsidiary of Cisco Systems.

11. On information and belief, Meraki maintains regular and established places of business and does business in Texas and in the Western District of Texas, *inter alia*, at Cisco's campus at 12515-3 Research Park Loop, Austin, TX 78759. As of April 7, 2020, Meraki has four job openings for its Austin location, including positions related to Engineering and Sales. *See*

https://jobs.cisco.com/jobs/SearchJobs/meraki?3_143_3=%5B%2212229489%22%5D&3_143_3_format=6021 (last visited 4/7/2020).

12. By registering to conduct business in Texas and by having facilities where it regularly conducts business in this District, Meraki has a permanent and continuous presence in Texas and a regular and established place of business in the Western District of Texas.

13. On information and belief, Defendant Duo is a corporation organized under the laws of Delaware with its principal place of business at 123 N. Ashley St. #100, Ann Arbor, Michigan 48104. Duo is registered to do business in the state of Texas. Duo has appointed C T Corporation System, 1999 Bryan St. Suite 900, Dallas, TX 75201 as its agent for service of process. Defendant Duo was acquired by and is a subsidiary of Cisco Systems.

14. On information and belief, Duo maintains regular and established places of business and does business in Texas and in the Western District of Texas, *inter alia*, at offices at 804 Congress Ave. Suite 500, Austin, TX 78701. As of April 7, 2020, Duo has 27 job openings for its Austin location, including positions related to Business Development, Customer Experience, Software Engineering, Marketing/Communications, and Sales. See https://jobs.cisco.com/jobs/SearchJobs/Duo%20Security?3_143_3=%5B%2212229489%22%5D&3_143_3_format=6021 (last visited 4/7/2020).

15. By registering to conduct business in Texas and by having facilities where it regularly conducts business in this District, Duo has a permanent and continuous presence in Texas and a regular and established place of business in the Western District of Texas.

JURISDICTION

16. This is an action arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq*. Accordingly, this Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

17. This Court has personal jurisdiction over Cisco Systems due, *inter alia*, to its continuous presence in, and systematic contact with, this judicial district and its registration in Texas and domicile in this judicial district. Cisco Systems is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State

and judicial district, including at least part of its past infringing activities, regularly doing or soliciting business at its Austin and San Antonio facilities, and engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in the State of Texas, including in the Western District of Texas. Cisco Systems directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this judicial district by, among other things, making, using, importing, offering for sale, and/or selling products and/or services that infringe the Asserted Patents.

18. This Court has personal jurisdiction over Meraki due, *inter alia*, to its continuous presence in, and systematic contact with, this judicial district and its registration in Texas and domicile in this judicial district. Meraki is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and judicial district, including at least part of its past infringing activities, regularly doing or soliciting business at its Cisco's Austin facility, and engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in the State of Texas, including in the Western District of Texas. Meraki directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this judicial district by, among other things, making, using, importing, offering for sale, and/or selling products and/or services that infringe the Asserted Patents.

19. This Court has personal jurisdiction over Duo due, *inter alia*, to its continuous presence in, and systematic contact with, this judicial district and its registration in Texas and domicile in this judicial district. Duo is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and judicial district, including at least part of its past infringing activities, regularly doing or soliciting business at its Austin facility, and engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in the State of Texas, including in the Western District of Texas. Duo directly and/or through subsidiaries or intermediaries (including distributors, retailers, and

others), has committed and continues to commit acts of infringement in this judicial district by, among other things, making, using, importing, offering for sale, and/or selling products and/or services that infringe the Asserted Patents.

VENUE

20. Venue is proper in this judicial district pursuant to 28 U.S.C. §§1391(b), (c), (d) and 1400(b) because Cisco Systems has a permanent and continuous presence in, has committed acts of infringement in, and maintains regular and established places of business in this district. Upon information and belief, Cisco Systems has committed acts of direct and indirect infringement in this judicial district, including using and purposefully transacting business involving the Cisco Accused Products in this judicial district such as by sales to one or more customers in the State of Texas, including in the Western District of Texas, and maintaining regular and established places of business in this judicial district, as set forth above.

21. Venue is proper in this judicial district pursuant to 28 U.S.C. §§1391(b), (c), (d) and 1400(b) because Meraki has a permanent and continuous presence in, has committed acts of infringement in, and maintains regular and established places of business in this district. Upon information and belief, Meraki has committed acts of direct and indirect infringement in this judicial district, including using and purposefully transacting business involving the Cisco Accused Products in this judicial district such as by sales to one or more customers in the State of Texas, including in the Western District of Texas, and maintaining regular and established places of business in this judicial district, as set forth above.

22. Venue is proper in this judicial district pursuant to 28 U.S.C. §§1391(b), (c), (d) and 1400(b) because Duo has a permanent and continuous presence in, has committed acts of infringement in, and maintains regular and established places of business in this district. Upon information and belief, Duo has committed acts of direct and indirect infringement in this judicial district, including using and purposefully transacting business involving the Cisco Accused Products in this judicial district such as by sales to one or more customers in the State of Texas,

including in the Western District of Texas, and maintaining regular and established places of business in this judicial district, as set forth above.

FACTUAL ALLEGATIONS

The ’507 Patent

23. The ’507 patent was invented by Siemens in Germany, which was a leader and pioneer in the areas of networking specific to this patent.

24. The ’507 Patent, entitled “Method and Device for Authenticated Access of a Station to Local Data Networks in Particular Radio Data Networks,” was duly and lawfully issued on July 13, 2010. Monarch is the owner of all right, title, and interest in the ’507 Patent. The ’507 Patent was filed on October 24, 2002 as Application No. 10/493,489 and claims priority to International Application No. PCT/EP02/11910, which was published in the German language on May 1, 2003, which claims the benefit of German Application No. 101 52 572.9 and European Application No. 011 25257.4, both filed on October 24, 2001. A true and correct copy of the ’507 Patent is attached hereto as Exhibit A.

25. The ’507 Patent is directed to a system and method for controlling and authenticating access to a local data network, such as a wireless local area network (WLAN). These wireless local area networks typically include one or more access points through which registered wireless computer devices connect to the network. A disadvantage of these types of local area networks is that they lack an authentication facility to control access to the network for computer devices that are not already registered in the system. The ’507 Patent provides a significant technological and security enhancement by providing authenticated access to a local area network (LAN) for computers and other devices that have a wireless interface to the LAN but which require authentication to connect or to continue to connect to the LAN. Rather than using the LAN itself as the medium for performing the authentication, the ’507 Patent makes use of a separate secure communication network, such as a mobile communications network that already includes sophisticated authentication facilities, as the network through which authentication occurs. Thus, to determine the authenticity of a computer device attempting to connect to a LAN, characteristic

information is transmitted over a secure path to a device such as a mobile phone that is external to the LAN, which may for example take the form of an SMS message or passcode that is delivered to the mobile phone. The characteristic information received on the mobile phone then is transferred or otherwise used to authenticate the computer device attempting to access the LAN. To implement the method disclosed by the ’507 Patent, the LAN may be associated with an access control unit that generates an identifier and transmits it via the secure communication network to another subscriber device, which then operates to authenticate the computer device seeking to connect to the LAN’s access point, without requiring any other modification to the secure communications network. By combining together the functionality of the two disparate networks – the LAN and the mobile communication network – the ’507 Patent provides a simple but elegant mechanism for authenticating computer devices attempting to connect to a LAN.

Cisco’s Use of the Patented Technology

26. Cisco’s Meraki Cloud Hosted Authentication supports an authentication method for wireless network clients to access resources or services connected to the data network through Meraki MR series WLAN access points. The Meraki authentication method implements one or more claims of the ’507 Patent. Thus, Cisco’s making, using, and selling of devices that implement and support its Meraki Cloud Hosted Authentication infringe one or more claims of the ’507 Patent.

27. Cisco Systems acquired the Meraki Cloud Hosted Authentication solution when it acquired Meraki, Inc. at the end of 2012. On information and belief, the Meraki Cloud Hosted Authentication solution is developed and supported by Cisco Systems’ subsidiary, Defendant Meraki. The Meraki Cloud hosted Authentication solution is marketed and sold by Cisco Systems.

28. Cisco’s Duo Security supports an authentication method for wireless network clients to access resources or services connected to the data network through a protected VPN or web application. The Duo Security authentication methods implement one or more claims of the ’507 Patent. Thus, Cisco’s making, using, and selling of software applications that implement and support its Duo Security infringe one or more claims of the ’507 Patent.

29. Cisco Systems acquired the Duo Security solution when it acquired Duo Security, a privately-held company, in 2018. On information and belief, the Duo Security solution is developed and supported by Cisco Systems' subsidiary, Defendant Duo. The Duo Security solution is marketed and sold by Cisco Systems, and in fact, is affirmatively marketed by Cisco Systems as part of its Cybersecuirty platform of products. *See* https://www.cisco.com/c/en/us/products/security/index.html#~why-cisco; https://www.cisco.com/c/en/us/products/security/adaptive-multi-factor-authentication.html.

30. Instrumentalities that include or use Cisco's Meraki Cloud Hosted Authentication and/or Cisco's Duo Security are collectively referred to as the "Cisco Accused Products."

FIRST COUNT

(Infringement of U.S. Patent No. 7,756,507)

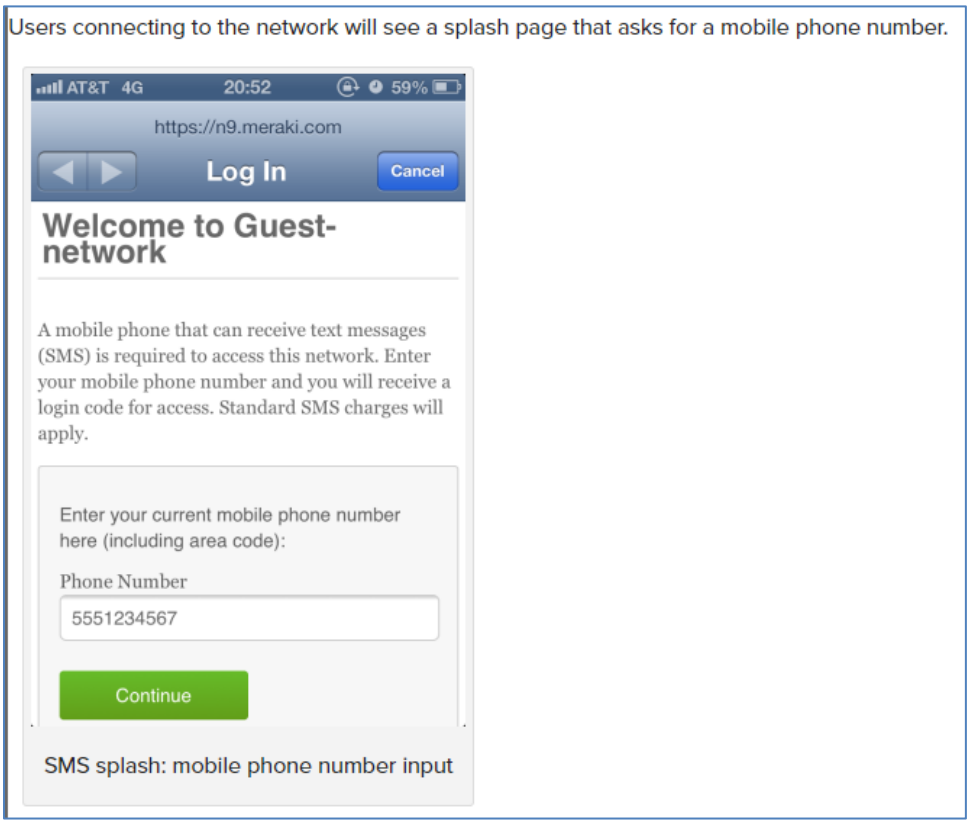
31. Monarch incorporates by reference the allegations set forth in Paragraphs 1-30 of this Complaint as though fully set forth herein.

32. Cisco makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that directly infringe the '507 Patent, including the above identified Cisco Accused Products that incorporate or use Meraki Cloud Hosted Authentication and/or Duo Security. The Cisco Accused Products infringe at least claim 1 of the '507 Patent.

33. Certain Cisco Accused Products implement Meraki Cloud Hosted Authentication, which supports an authentication method for wireless network clients to access the resources or services connected to the data network through WLAN access points, including at least the Meraki MR series WLAN access points and Meraki MX series products.

https://documentation.meraki.com/MR (last visited 1/14/2020).

34. Using the Splash page sign-on, users transmit identification information to the Meraki access point.

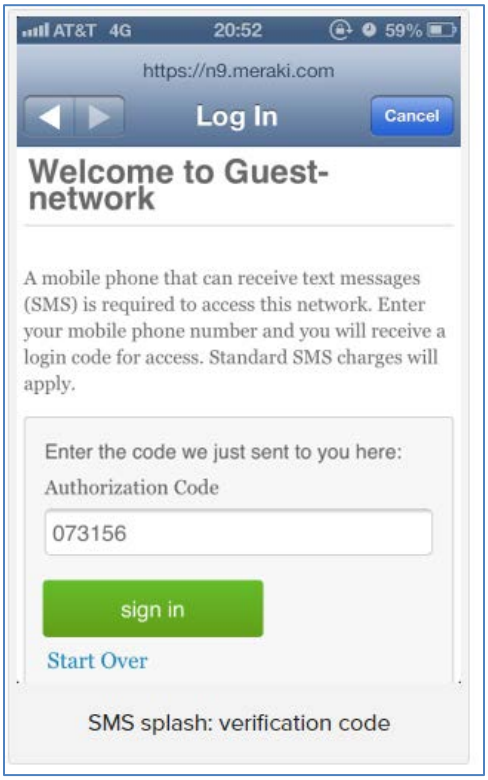


https://meraki.cisco.com/blog/tag/guest-wireless/ (last visited 1/14/2020). The identification information transmitted to the Meraki AP is a mobile phone number.

35. The Cisco Accused Products then provide and transmit a password via an interface to an authenticated device of a system or network external to the access point, having an authenticating function. A login or verification code is sent to the mobile phone provided as the identification

information. The mobile phone acts as an authenticated device external to the Meraki AP providing the authenticating function. https://meraki.cisco.com/blog/tag/guest-wireless/ (last visited 1/14/2020) ("Meraki's system then sends a verification code via text message to the mobile number, and the user enters the code into the splash page to get access to the network.").

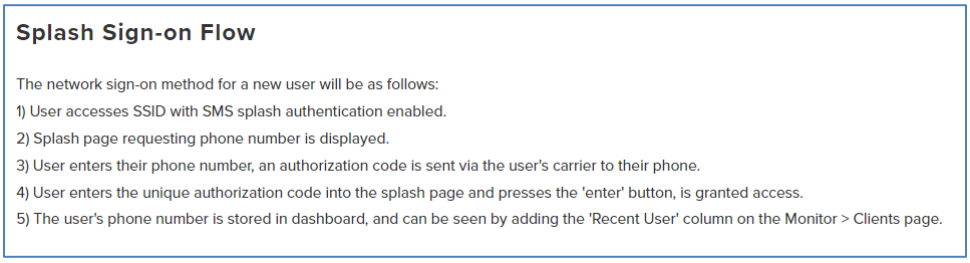
36. Additionally, the identification information is directly assigned to the device authenticated in the external system or network and access to data of the authenticated device is available at a location of the station or of the access point. The identification information is the mobile phone number to which the verification code is sent. The mobile phone's data is accessible at a location of the client, where the client enters the received code into the splash page.



https://meraki.cisco.com/blog/tag/guest-wireless/ (last visited 1/14/2020).

37. Once the client enters the verification code into the splash page, the code is then transmitted to the Meraki AP. On receipt, the Meraki AP compares the verification code received to the code sent to the mobile phone to determine whether the client is granted access to the network. If the

codes match, the client is granted access to at least some services and functions at the access-point end or at the network end.



Splash Sign-on Flow

The network sign-on method for a new user will be as follows:
1) User accesses SSID with SMS splash authentication enabled.
2) Splash page requesting phone number is displayed.
3) User enters their phone number, an authorization code is sent via the user's carrier to their phone.
4) User enters the unique authorization code into the splash page and presses the 'enter' button, is granted access.
5) The user's phone number is stored in dashboard, and can be seen by adding the 'Recent User' column on the Monitor > Clients page.

https://documentation.meraki.com/MR/MR_Splash_Page/Splash_Page_Details_for_Meraki_MR (last visited 1/14/2020).

38. Certain Cisco Accused Products implement Duo Security, which supports an authentication method service for controlling the access of client devices (stations) to a data network, such as Virtual Private Networks (VPN's) and other cloud or Internet based services.

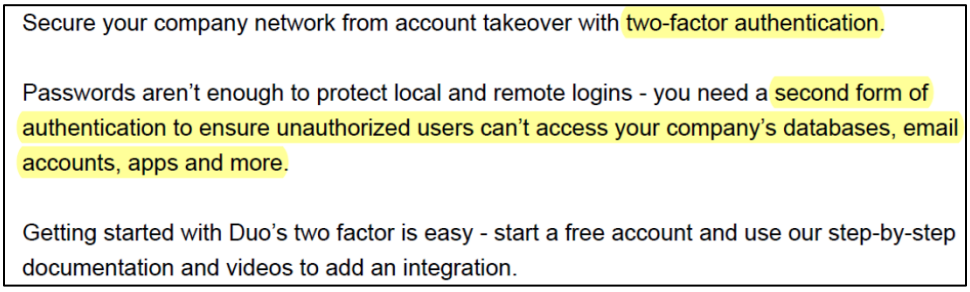
Duo Security is a vendor of cloud-based two-factor authentication services.

Duo's service is free for personal use (up to 10 users); additional options are available for business and enterprise users. Duo's two-factor authentication system can be integrated with websites, VPNs and cloud services. The service can be set to work in conjunction with smartphones, personal computers, land lines and security tokens.

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Two-factor authentication increases the security of online communications by making it harder for a hacker to masquerade as an authorized user. Duo's authentication factors are the user name and password (something the user knows) and a device (something the user has). A hacker may be able to steal or guess the user name and password but without verification from the user's device will not be able to use the login information.

Here's an example of how Duo's two-factor authentication works: A website user logs into his account and accepts the option to sign up for the service. When he visits the site next he enters his username and password as usual. Duo sends a message to the smartphone or other device associated with that account; the response verifies the user's identity.

https://searchsecurity.techtarget.com/definition/Duo-Security (last visited 4/7/2020).



Secure your company network from account takeover with two-factor authentication.

Passwords aren't enough to protect local and remote logins - you need a second form of authentication to ensure unauthorized users can't access your company's databases, email accounts, apps and more.

Getting started with Duo's two factor is easy - start a free account and use our step-by-step documentation and videos to add an integration.

https://duo.com/resources/videos/protect-your-network-with-two-factor-authentication (last visited 4/7/2020).

Enrolling Your Phone or Tablet in Duo

Duo prompts you to enroll the first time you log into into a protected VPN or web application when using a browser or client application that shows the interactive Duo web-based prompt. Alternatively, you might receive an email from your organization's Duo administrator with an enrollment link.

Supported Browsers: Chrome, Firefox, Safari, Edge, Opera, and Internet Explorer 8 or later. Some browsers do not support all of Duo's authentication devices (for example, Security Keys won't work with Internet Explorer). For the widest compatibility with Duo's authentication methods, we recommend recent versions of Chrome and Firefox.

https://guide.duo.com/enrollment (last visited 4/7/2020).

What is Two-Factor Authentication?

Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a **second factor** (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password.

https://guide.duo.com/ (last visited 4/7/2020).

How It Works

1. **Enter username and password as usual**
2. **Use your phone to verify your identity**
3. **Securely logged in**

Once you've enrolled in Duo you're ready to go: You'll login as usual with your username and password, and then use your device to verify that it's you. Your administrator can set up the system to do this via SMS, voice call, one-time passcode, the Duo Mobile smartphone app, and so on.

No mobile phone? You can also use a landline or tablet, or ask your administrator for a hardware token. Duo lets you link multiple devices to your account, so you can use your mobile phone and a landline, a landline and a hardware token, two different mobile devices, etc.

https://guide.duo.com/ (last visited 4/7/2020).

> Duo Security provides two-factor authentication as a service to protect against account takeover and data theft. Using the Duo plugin you can easily add Duo two-factor authentication to your WordPress website in just a few minutes!
>
> Rather than relying on a password alone, which can be phished or guessed, Duo's authentication service adds a second layer of security to your WordPress accounts. Duo enables your admins or users to verify their identities using something they have—like their mobile phone or a hardware token—which provides strong authentication and dramatically enhances account security.

https://wordpress.org/plugins/duo-wordpress/ (last visited 4/7/2020).

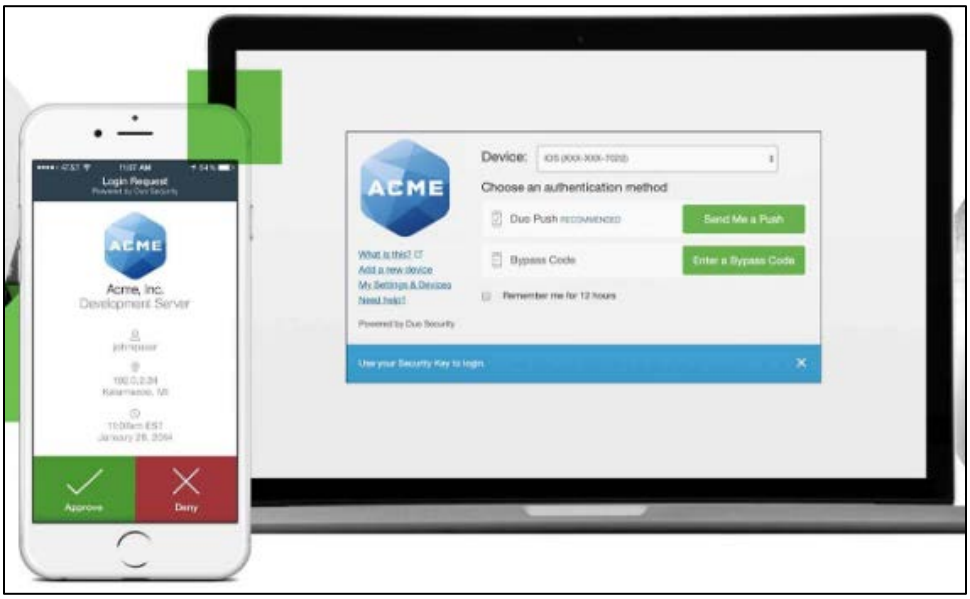
> Typically, a 2FA transaction happens like this:
>
> 1. The user logs in to the website or service with their username and password.
> 2. The password is validated by an authentication server, and if correct, the user becomes eligible for the second factor.
> 3. The authentication server sends a unique code to the user's second-factor device.
> 4. The user confirms their identity by approving the additional authentication from their second-factor device.

https://duo.com/blog/two-factor-authentication-the-basics (last visited 4/7/2020).

> Duo secures your workforce
>
> Duo Security helps protect your users and their devices against stolen credentials, phishing, and other identity-based attacks. It verifies users' identities and establishes device trust before granting access to applications.

https://www.cisco.com/c/en/us/products/security/zero-trust.html#~solutions (last visited 4/7/2020).

39. Duo Security connects to the network and transmit identification information in the form of a user name and password to the network server.



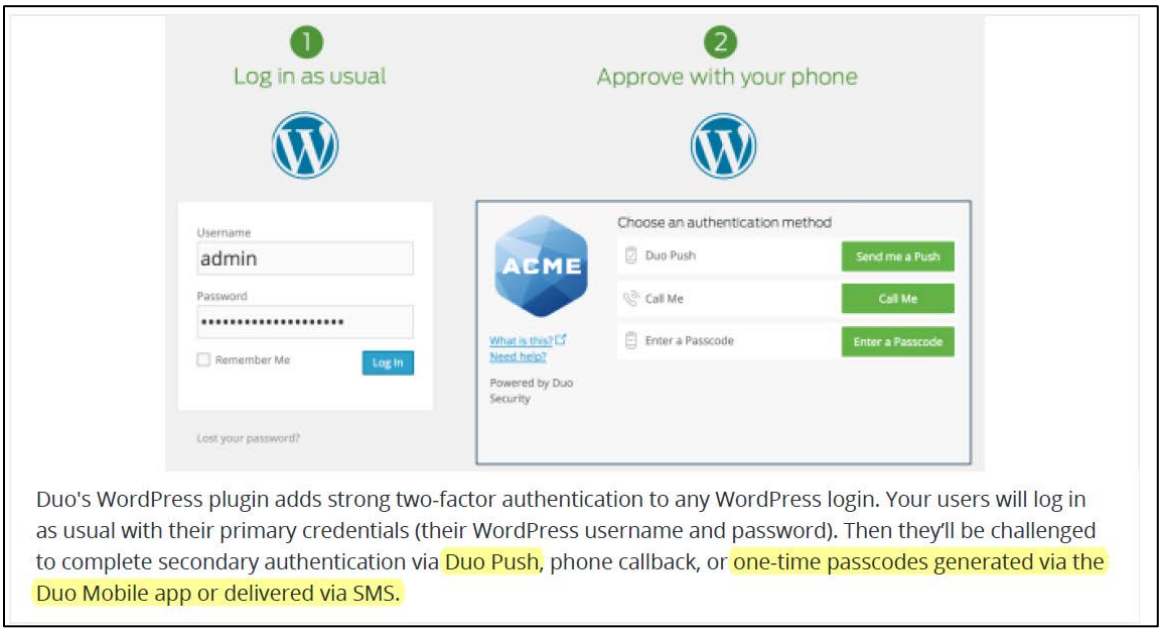
https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa (last visited 4/7/2020).

> Let's say you use a username and password to complete primary authentication to an application. That information is sent over the Internet (your primary network). You'll want to use a different (out-of-band) channel to complete your second factor. Approving a push notification sent over your mobile network is an example of out-of-band authentication.

Id.

40. Also, when enrolling a mobile phone or tablet as a second factor authentication device for access to a data network, the user enters the phone number of the mobile phone or tablet to identify that device and the device is associated with that user's Duo account. *See* https://guide.duo.com/enrollment. Enrolled devices are associated with specific Duo user accounts. *See* https://duo.com/docs/administration-devices.

41. Duo Security can be configured so that an authorization code is sent via a mobile network to an authenticated mobile phone or tablet. The mobile phone acts as an authenticated external device to the network providing the authenticating function.



https://wordpress.org/plugins/duo-wordpress/ (last visited 4/7/2020).

42. According to one implementation, a barcode may be sent to a mobile phone that is used to activate the Duo Mobile app on the mobile phone. The mobile phone is external to the data network being accessed.

https://guide.duo.com/enrollment (last visited 4/7/2020).

43. As another alternative, the Duo Mobile app may be activated by receiving an activation link via an SMS message that is either clicked to activate or the link is pasted into the Duo Mobile app to activate it.

> To activate Duo Mobile when the SMS activation link will not open, follow these steps:
>
> 1. Send a new activation SMS to the user's phone. The user should not click on the link in the SMS.
> 2. Copy the entire activation link from the SMS (e.g. https://m-xxxx.duosecurity.com/android/yyyyyyy)
> 3. Open Duo Mobile.
> 4. Click the new account button at the top (key icon with '+' sign).
> 5. Under the camera view, click **No Barcode?**.
> 6. Select **Duo Security Enabled Account**.
> 7. Paste the entire activation link into the text field.
> 8. Press the the checkmark at the top right of the app, or the phone keyboard's **Return** button, to submit the activation link.

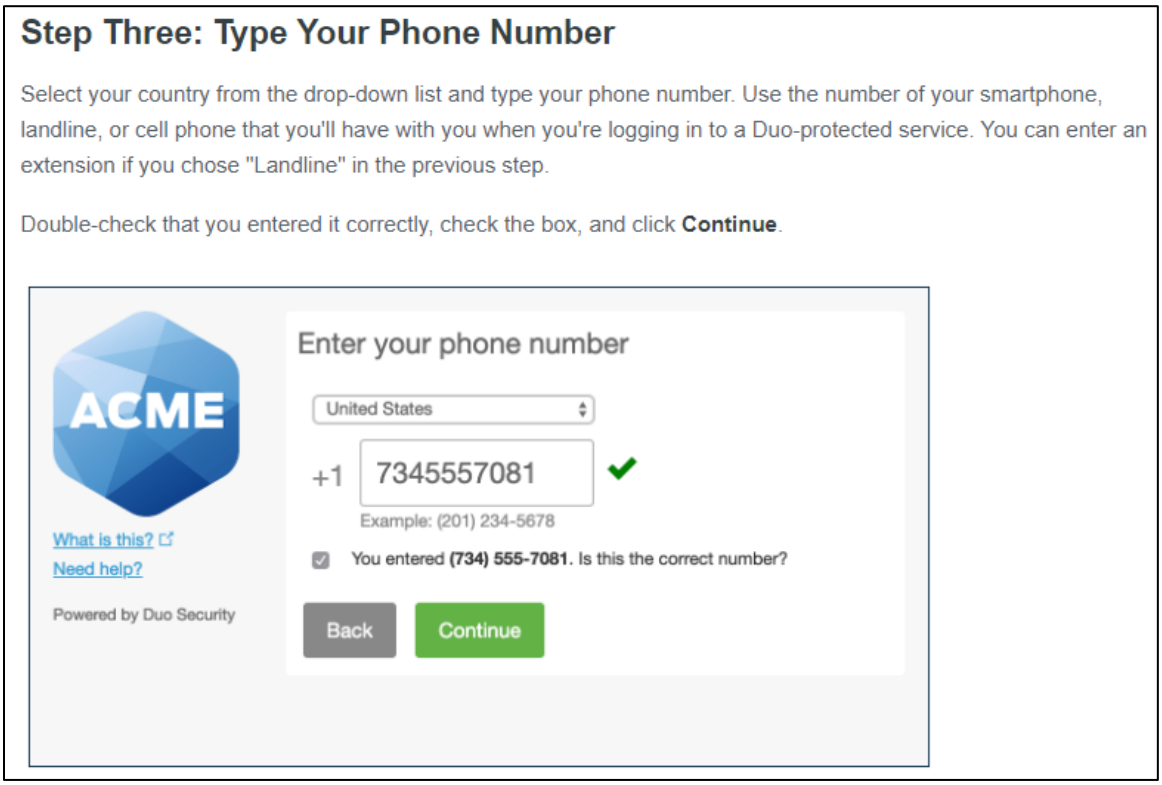
https://help.duo.com/s/article/3664?language=en_US (last visited 4/7/2020).

44. The username and password are associated with a user's phone that is external to the network, and the data sent to the phone is used to authenticate the user's computer seeking to access the network.

> When they log in, your users have multiple ways they can authenticate, including:
>
> - One-tap authentication using Duo's mobile app (our fastest, easiest way to authenticate)
> - One-time passcodes generated by Duo's mobile app (works even with no cell coverage)
> - One-time passcodes delivered to any SMS-enabled phone (works even with no cell coverage)
> - Phone callback to any phone (mobile or landline!)
> - One-time passcodes generated by an OATH-compliant hardware token (if you're feeling all old school)

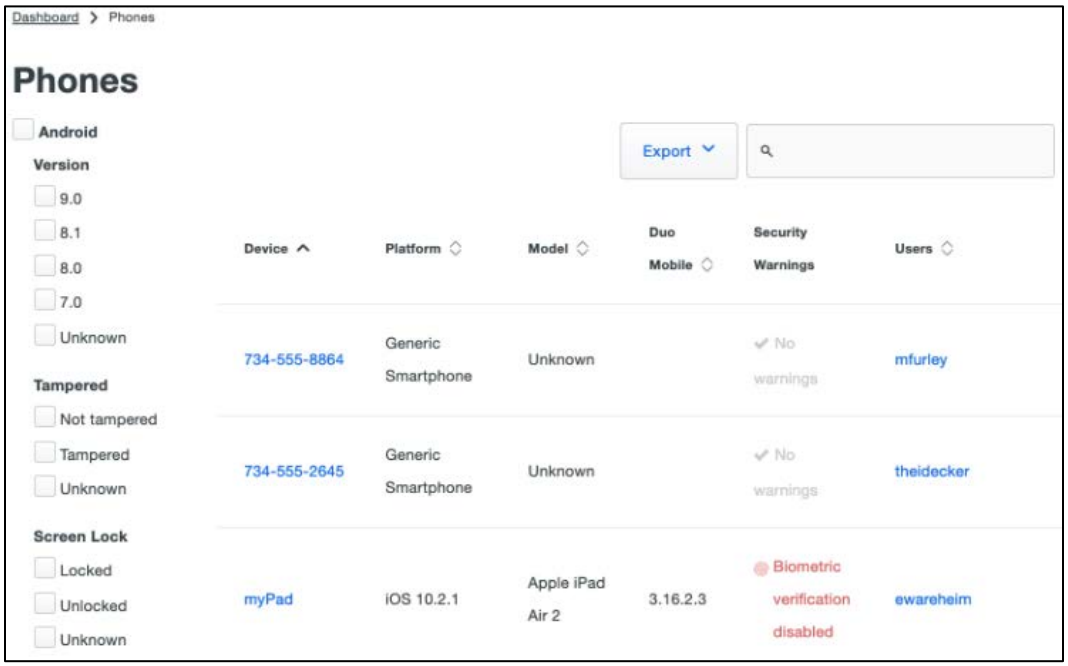
https://wordpress.org/plugins/duo-wordpress/ (last visited 4/7/2020).

45. When enrolling a mobile phone or tablet as a second factor authentication device for access to a data network, the user enters the phone number of the mobile phone or tablet itself to identify that mobile device.



https://guide.duo.com/enrollment#enter-your-phone-number (last visited 4/7/2020).

46. 2FA devices (e.g., mobile phones, tablets) are associated with a Duo user account.



https://duo.com/docs/administration-devices (last visited 4/7/2020).

47. The password sent to the mobile phone is used to authenticate the computer device seeking to access the network. *See* https://wordpress.org/plugins/duo-wordpress/

> SMS two-factor authentication validates the identity of a user by texting a security code to their mobile device. The user then enters the code into the website or application to which they're authenticating.

> The Time-Based One Time Password (TOTP) 2FA method generates a key locally on the device a user is attempting to access. The security key is generally a QR code that the user scans with their mobile device to generate a series of numbers. The user then enters those numbers into the website or application to gain access. The passcodes generated by authenticators expire after a certain period of time, and a new one will be generated the next time a user logs in to an account. TOTP is part of the Open Authentication (OAUTH) security architecture.

> Push-based 2FA improves on SMS and TOTP 2FA by adding additional layers of security, while improving ease of use for end users. Push-based 2FA confirms a user's identity with multiple factors of authentication that other methods cannot. Duo Security is the leading provider of push-based 2FA.
>
> **Pros**
>
> - **Phishing security.** Other types of two factor authentication are susceptible to phishing attacks, but push-based 2FA combats that vulnerability by replacing access codes with push notifications. When they attempt to access their information, a push notification is sent to the user's phone. The notification includes information about the login attempt, such as location, time, IP address, and more. The user simply confirms that the information is correct and uses their phone to accept the authentication request.

https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa (last visited 4/7/2020).

48. Duo Security generates an encoded key that is transferred to the authenticated device and back from that authenticated device to the station. Such keys are based on iKeys, sKeys, and/or aKeys. *See* https://help.duo.com/s/article/3664?language=en_US. Use of these keys are illustrated by SignRequest() and VerifyResponse() functions provided for DuoWeb. https://github.com/duosecurity (DuoWeb.cs).

49. The verification code sent to the mobile phone and the verification code received by the authentication server are compared to grant the client access to the network. *See*

https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa (last visited 4/7/2020)

50. By making, using, offering for sale, and/or selling products in the United States, and/or importing products into the United States, including but not limited to the Cisco Accused Products, Cisco has injured Monarch and is liable to Monarch for directly infringing one or more claims of the ’507 Patent, including without limitation claim 1 pursuant to 35 U.S.C. § 271(a).

51. Cisco also indirectly infringes the ’507 Patent under 35 U.S.C. § 271(b) & (c).

52. Cisco knowingly encourages and intends to induce infringement of the ’507 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the Cisco Accused Products, with knowledge and specific intention that such products will be used by its customers. For example, Cisco instructs its customers on how to use and implement the technology claimed in the ’507 patent. *See, e.g.*, Meraki and Duo Websites cited supra.

53. Cisco also contributes to the infringement of the ’507 Patent. Cisco makes, uses, sells, and/or offers to sell products in the United States, and/or imports them into the United States, including but not limited to the Cisco Accused Products, knowing that those products constitute a material part of the claimed invention, that they are especially made or adapted for use in infringing the ’507 Patent, and that they are not staple articles or commodities of commerce capable of substantial non-infringing use.

54. As a result of Cisco’s infringement of the ’507 Patent, Monarch has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Cisco’s infringement, but in no event less than a reasonable royalty with interest and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment and seeks relief against Cisco as follows:

(a) For judgment that U.S. Patent No. 7,756,507 has been and continues to be infringed by Cisco;

(b) For an accounting of all damages sustained by Plaintiff as the result of Cisco's acts of infringement;

(c) For finding that Cisco's infringement is willful and enhancing damages pursuant to 35 U.S.C. § 284;

(d) For a mandatory future royalty payable on each and every future sale by Cisco of a product that is found to infringe one or more of the Asserted Patents and on all future products which are not colorably different from products found to infringe;

(e) For an award of attorneys' fees pursuant to 35 U.S.C. § 285 or otherwise permitted by law;

(f) For all costs of suit; and

(g) For such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff demands a trial by jury of this action.

Dated: May 13, 2020

Respectfully Submitted,

/s/ Max L. Tribble

Max L. Tribble Jr.
Texas Bar No. 20213950
mtribble@susmangodfrey.com
Joseph S. Grinstein
Texas Bar No. 24002188
jgrinstein@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, Texas 77002
Telephone: (713) 651-9366
Facsimile: (713) 654-6666

Steven M. Shepard
New York Bar No. 5291232
sshepard@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas 32nd Floor
New York, NY 10019
Telephone: (212) 336-8330

Facsimile: (212) 336-8340

Michael F. Heim
Texas Bar No. 09380923
mheim@hpcllp.com
R. Allan Bullwinkel
Texas Bar No. 24064327
abullwinkel@hpcllp.com
Alden G. Harris
Texas Bar No. 24083138
aharris@hpcllp.com
HEIM, PAYNE & CHORUSH, LLP
1111 Bagby St. Ste. 2100
Houston, Texas 77002
Telephone: (713) 221-2000
Facsimile: (713) 221-2021

T. John Ward, Jr.
Texas Bar No. 00794818
E-mail: jw@wsfirm.com
Claire Abernathy Henry
Texas Bar No. 24053063
E-mail: Claire@wsfirm.com
WARD, SMITH & HILL, PLLC
1507 Bill Owens Pkwy.
Longview, Texas 75604
Telephone: (903) 757-6400
Facsimile: (903) 757-2323

S. Calvin Capshaw, III
Texas Bar No. 03783900
Capshaw DeRieux LLP
114 E. Commerce Avenue
Gladewater, TX 75647
Phone: (903) 845-5770
Email: ccapshaw@capshawlaw.com

ATTORNEYS FOR MONARCH NETWORKING SOLUTIONS LLC